SPRINGFIELD OREGON	**Administrative Regulation** **Information & Cyber Security**	**Policy #**	04.02.01
		Effective Date:	October 1, 2020
		Revision Date:	N/A
		Owner:	Information Technology

Purpose:

The purpose of this policy is to clearly communicate City of Springfield cybersecurity objectives and guidelines to establish a security oriented culture and minimize the risk of internal and external threats while taking advantage of opportunities that promote our strategic objectives.

Scope:

This regulation applies to all City of Springfield elected officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the City of Springfield.

The information presented in this administrative regulation follows the control families outlined in the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF): Identify, Protect, Detect, Respond, and Recover. The scope of security controls addressed in this policy focus on the activities most relevant to the City of Springfield as defined by the Center for Internet Security (CIS) and industry best practices. Additionally, leadership must ensure that all contracts and similar agreements with business partners and service providers incorporate appropriate elements of this policy

Policy:

The City of Springfield will comply with the Oregon Identity Theft Protection Act, ORS 646A.600 – 628. ORS 646A.622 (d) requires the implementation of a Cybersecurity program. Non-compliance with this policy may pose risks to the City as an organization. Accordingly, compliance with this program is mandatory. Failure to comply may result in failure to obtain organizational objectives, legal action, fines and penalties issued to the City. Breaches with the potential to impact more than 250 individuals must be reported to the Oregon Department of Justice.

Procedure: *This section outlines the City's requirements and minimum standards to facilitate the secure use of the City's information systems.*

1. Asset Management

    1.1. An inventory of all approved hardware and software on the City of Springfield network and systems will be maintained by the IT Department in a computer program or spreadsheet that documents the following:

- The employee in possession of the hardware or software;
- Date of purchase;
- Serial number;
- Type of device and description; and
- A listing of software or devices that have been restricted.

2. Personally Identifiable Information (PII)

2.1. IT will initiate an annual update to compile and inventory all PII by type and location.

2.2. Department directors will coordinate with IT or Risk Management to determine if PII is essential. If PII is not essential, it will either not be collected, or (if previously collected) will be destroyed, subject to requirements of the Oregon Public Records Law and the City's Records Retention and Destruction Policy.

2.3. All PII no longer needed shall be shredded by departments if in paper form or destroyed by IT if in electronic form, according to requirements of the Oregon Public Records Law and the City's Records Retention and Destruction Policy.

3. The Oregon Identity Theft Protection Act

3.1. Unless exempted by State or Federal law, the City will comply with the Oregon Identity Theft Protection Act by prohibiting anyone from:

3.1.1. Printing a consumer's Social Security Number (SSN) on any mailed materials not requested by the consumer unless redacted;

3.1.2. Printing a consumer's SSN on a card used by the consumer that is required to access products or services; and

3.1.3. Publicly posting or displaying a consumer's SSN, such as on a website.

4. Identity Management, Authentication and Access Control

4.1. The Network Manager or designee is responsible for ensuring that access to the City's systems and data is appropriately controlled.

4.2. Wherever possible, systems housing City of Springfield data (including laptops, desktops, tablets, and cell phones) are required to be protected with a password or other form of authentication. Except for the instances noted in this policy, users with access to City of Springfield systems and data are not to share passwords with anyone.

4.3. Where applicable, the City of Springfield has established the following password configuration requirements for all systems and applications:

- Minimum password length: 8 characters;

- Password complexity: requires alphanumeric and special characters;
- Prohibited reuse for a minimum of four (4) iterations;
- Changed periodically every 90 days;
- Invalid login attempts set to three; and
- Automatic logout due to inactivity after 30 minutes.

4.4. Other potential safeguards include:

- Not allowing PII on mobile storage media;
- Locking file cabinets;
- Not allowing PII to be left on desks;
- Encrypting sensitive files on computers;
- Requiring password protection; and
- Implementing the record retention plan and destroying records no longer required

4.5. Where possible, multi-factor authentication will be used when users access the City's systems.

4.5.1. Users are granted access only to the system data and functionality necessary for their job responsibilities.

4.5.2. Privileged and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts: one for administrator functions and a standard account for day-to-day activities.

4.5.3. All user access requests must be approved by the Network Manager or their designee.

4.5.4. It is the responsibility of the Network Manager or their designee to ensure that all employees and contractors who separate from the organization have all system access removed within twenty four (24) hours' notice.

4.5.5. On an annual basis, a review of user access will be conducted by the IT department under the direction of the Network Manager or designee to confirm compliance with the access control policies outlined above.

5. Awareness and Training

5.1. The City will strive to implement the following trainings:

5.1.1. *Initial Hire Training:* All new hires are required to complete security awareness training before receiving login credentials. Upon completion of training, participants will review and sign the Acceptable Use of City Network Services & Computing Devices Administrative Regulation form.

5.1.2. *Annual Training:* Formal security awareness refresher training is conducted on an annual basis. All employees are required to participate in and complete this training.

5.2. The City of Springfield will conduct annual email phishing exercises. The purpose of these tests is to help educate users on common phishing scenarios. It will assess their level of awareness and comprehension of phishing, understanding and compliance with policy around safe handling of e-mails containing links and/or attachments, and their ability to recognize a questionable or fraudulent message.

6. Data Security

6.1. *Data Classification.* Data residing on City systems must be continually evaluated by the IT Department and classified into the following categories:

6.1.1. *Employees Personal Use:* Includes individual user's personal data, emails, documents, etc. This policy excludes an employee's personal information, so no further guidelines apply.

6.1.2. *Marketing or Informational Material:* Includes already-released marketing material, commonly-known information, data freely available to the public, etc. There are no requirements for public information.

6.1.3. *Operational:* Includes data for basic organizational operations, communications with vendors, employees, etc. that are not confidential. The majority of data will fall into this category.

6.1.4. *Confidential:* Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:

- Employee or customer SSN or personally identifiable information (PII);
- Personnel files;
- Medical and healthcare information;
- Protected Health Information (PHI);
- Network diagrams and security configurations;
- Communications regarding legal matters;
- Passwords/passphrases;
- Bank account information and routing numbers;
- Payroll information;
- Credit card information; and
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information).

6.2. *Data Storage Types*.

6.2.1. The following guidelines apply to storage of the different types of organizational data:

- *Operational:* Operational data should be stored on a server that gets the most frequent backups. Some type of system- or disk-level redundancy is encouraged.

- *Confidential:* Confidential information must not be left in the open, on computer screens, and in common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard or code secured.

6.3. *Data Transmission.*

6.3.1. The following guidelines apply to the transmission of the different types of organizational data. Wherever possible, confidential data must not be:

- Transmitted outside the organization's network without the use of strong encryption.

- Left on voicemail systems, either inside or outside the organization's network.

6.4. *Data Destruction*.

6.4.1. City users will follow the City’s Records Retention and Destruction administrative regulation before destroying data. Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: Cross-cut shredding is required.

- Storage media (CD's, DVD's): Physical destruction is required.

- Hard drives/systems/mobile storage media: At a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the organization must use the most secure commercially-available methods for data wiping. Alternatively, the organization has the option of physically destroying the storage media.

6.5. *Data Storage and Transmission*

6.5.1. Stored data located on organization-owned or organization-provided systems, devices, media, etc., will be encrypted when possible. Examples of encryption options include:

- Whole disk encryption;
- Encryption of partitions/files;
- Encryption of disk drives;
- Encryption of personal storage media/USB drives;
- Encryption of backups; and
- Encryption of data generated by applications.

6.5.2. Data being transmitted across the organization network or any data sent to or from an organization-owned or organization-provided system shall be encrypted when possible. This includes but is not limited to:

- VPN tunnels;
- Remote access sessions;
- Web applications;
- Email and email attachments;
- Remote desktop access; and
- Communications with applications/databases.

7. Information Protection Processes and Procedures

7.1. *Secure Software Development.*

7.1.1. Where applicable, all software development activities performed by the City of Springfield or by vendors on behalf of the City shall employ secure coding practices including those outlined below.

7.1.2. Where feasible, the City will use development, quality assurance and production environments when developing software systems. Software developers or programmers will develop in the development environment and promote objects into the quality assurance and production environment. The quality assurance environment will be used for assurance testing by the end user and the developer. The production environment should be used solely by the end user for production data and applications. Compiling objects and the source code is not allowed in the production environment.

- All production changes must be approved before being promoted to production.

- All production changes must have a corresponding help desk change request number.

- All production changes should be developed in the development/test environment.

- All emergency changes should be adequately documented and approved per IT department procedures.

7.2. *Contingency Planning*

7.2.1. The City's business contingency capability is based upon both Cloud and Local backups of all critical business data. Full data backups will be performed on at least a weekly basis by IT. The IT Department will confirm that backups were performed successfully will be conducted monthly. Testing of cloud backups and full restoration testing of critical system backups should be performed on an annual basis.

7.2.2. During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the IT Director or designee in connection with Risk Management, City Attorney's Office and City Manager's Office as required.

7.2.3. The following business contingency event scenarios have been identified along with the intended responses:

- In the event that one or more of the City of Springfield's systems or applications are deemed corrupted or inaccessible, the Network manager or designee will work with the respective vendor(s) to restore data from the most recent backup and, if necessary, acquire replacement hardware.

- In the event that the location housing the City of Springfield systems are no longer accessible, the Network Manager or their designee will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the organizations other sites, and restore data from the most recent backup.

7.3. *Network Infrastructure*

7.3.1. The City will protect the organization's electronic communications network from the Internet by utilizing a firewall. For maximum protection, the corporate network devices shall meet the following configuration standards:

- Vendor-recommended and industry standard configurations will be used.

- Changes to firewall and router configuration will be approved by the Network manager or designee.

- Both router and firewall passwords must be secured and difficult to guess.

- The default policy for the firewall for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted.

- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic should not be passed in from the Internet, or from any un-trusted external network.

- All web services running on routers must be disabled.

- Simple Network Management Protocol (SNMP) Community Strings must be changed from the default "public" and "private".

7.4. *Network Servers*.

7.4.1. The City will follow the following guidelines when possible:

- Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.

- Network servers, even those meant to accept public connections must be protected by a firewall or access control list.

- If possible, a standard installation process should be developed for the City's network servers. A standard process will provide consistency across servers no matter what employee or contractor handles the installation.

- Clocks on network servers should be synchronized with the City's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

7.5. *Network Segmentation*

7.5.1. Network segmentation is used to limit access to data within the City of Springfield network based upon data sensitivity. The City of Springfield maintains two wireless networks. The guest wireless will grant the user internet access only. Access to the secure wireless network is limited to City of Springfield personnel.

7.5.2. Under the direction of the Network Manager or their designee, Lane County IT manages the network user accounts, monitors firewall logs, and operating system event logs. The Network Manager or their designee authorizes vendor access to the system components as required for maintenance.

8. <u>Protective Technology</u>

8.1. *Email Filtering.*

8.1.1. The City of Springfield will filter email at the Internet gateway and/or the mail server to reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the organization's IT security. McAfee Quarantine Manager has been implemented to identify and quarantine emails that are deemed suspicious.

8.2. *Network Vulnerability Assessments*

8.2.1. The City will perform both internal and external network vulnerability assessments. These evaluations will be conducted under the direction of the Network Manager or their designee to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization's data and systems.

8.2.2. Penetration testing, which is the active exploitation of organization vulnerabilities, is discouraged. If penetration testing is performed, it must not negatively impact City systems or data.

9. Anomalies and Events

9.1. The following logging activities will be conducted under the direction of the Network manager or designee:

9.1.1. *Domain Controllers*: Active Directory event logs will be configured to log the following security events: account creation, escalation of privileges, and login failures.

9.1.2. *Application Servers*: Logs from application servers (e.g., web, email, database servers) will be configured to log the following events: errors, faults, and login failures.

9.1.3. *Network Devices*: Logs from network devices (e.g., firewalls, network switches, routers) will be configured to log the following events: errors, faults, and login failures.

9.2. Passwords should not be contained in logs.

9.3. The City will strive to implement tools to review the logs above.

10. Security Continuous Monitoring

10.1. *Anti-Malware Tools*

10.1.1. All City servers and workstations will utilize antivirus and malware software to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed. The Network Manager or their designee will review the dashboard monthly to confirm the status of virus definition updates and scans.

10.1.2. The City of Springfield will work toward using a tool to protect mobile devices from malware and viruses.

10.2. *Patch Management*

10.2.1. All software updates and patches will be distributed to all the City of Springfield system as follows:

- Workstations will be configured to install software updates automatically every month.

- Server software updates will be manually installed at least monthly.

- Any exceptions shall be documented.

11. Response Planning

11.1. The IT Department is responsible to conduct an annual security awareness training with all IT system users which shall include direction and guidance for the types of security incidents users could encounter (both physical and electronic), what actions to take when an incident is suspected, and who is responsible for responding to an incident.

11.2. The Network Manager or their designee is responsible for coordinating all activities during a significant incident, including notification and communication activities. They are also responsible for the chain of escalation and deciding if/when outside agencies, such as law enforcement, need to be contacted.

11.3. *Electronic Incidents*

11.3.1. When an electronic incident is suspected, the steps below should be taken in order:

11.3.1.1. Remove the compromised device from the network by unplugging or disabling network connection. **Do not power down the machine**.

11.3.1.2. Report the incident to the Network Manager or their designee and to the Risk Manager. The Network Manager or their designee will notify the third-party service provider (and/or computer forensic specialist) as needed

11.3.2. The remaining steps should be conducted with the assistance of a third-party IT service provider and/or computer forensics specialist:

11.3.2.1. Disable the compromised account(s) as appropriate.

11.3.2.2. Backup all data and logs on the machine, or copy/image the machine to another system.

11.3.2.3. Determine exactly what happened and the scope of the incident.

11.3.2.4. Determine how the attacker gained access and disable it.

11.3.2.5. Rebuild the system, including a complete operating system reinstall.

11.3.2.6. Restore any needed data from the last known good backup and put the system back online.

11.3.2.7. Take actions, as possible, to ensure that the vulnerability will not reappear.

11.3.2.8. Conduct a post-incident evaluation. What can be learned? What could be done differently?

11.4. *Physical Incidents.*

11.4.1. A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain organization information. All instances of a suspected physical security incident should be reported immediately to the Network Manager or their designee. In the case of suspected theft, incidents should also be reported to local law enforcement.

11.5. *Notification.*

11.5.1. If an electronic or physical security incident is suspected of having resulted in the loss of third-party/customer data, The Network Manager and Risk Manager will notify:

- Insurance
- City Attorney
- The department of Justice, using the breach notification forms if the breach involves more than 250 records.

12. <u>Recovery</u>

12.1. The Network Manager or their designee is responsible for managing and directing activities during an incident, including the recovery steps.

12.2. The Network Manager or their designee is responsible for identifying, evaluating, and incorporating lessons learned into future activities and policies.

12.3. Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of the affected systems, victims, and vendors.

12.4. External communications should only be handled by designated individuals at the direction of the Network Manager or their designee. Recovery activities are communicated to internal stakeholders, and the Executive Team.

Definitions

1. *“Leadership”* is any employee who guides or directs one or more employees.

2. *Personally Identifiable Information" (PII)* mean personal information as defined in the Oregon Consumer Information Protection Act at ORS 646.602(12). PII includes first name or initial with the last name together with any of the following: numbers that identify a consumer including social security, drivers’ license, state ID, passport, financial account, or payment card numbers; biometric data on a consumer’s physical characteristics, including fingerprints and eye scans; and health insurance or medical history information. PII also includes user names or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification. In addition, when data has not been encrypted and theft of the data would enable a person to be a victim of identity theft, any of the foregoing information can be considered PII even in absence of the user name or the combination of first and last name. PII does not include information in federal, state, or local government records lawfully made available to the public.

3. *"Protected Health Information" (PHI) is* as defined in the Health Insurance Portability and Accountability Act (HIPAA) regulations at 45 CFR 160.103. PHI includes information that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual, that is held or transmitted in any form by a covered entity or its business associate, as defined under HIPAA, and that relates to any of the following: the individual’s past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual.

Resources:

1. Acceptable Use of City Network and Computing Devices Administrative Regulation
2. Backup Policy (Pending)
3. Records Retention and Destruction Administrative Regulation
4. US Department of Justice Breach notification website

This administrative regulation is in effect as of the date of my signature. I authorize the Human Resource Director to modify the history and resources sections and header, footer, and numbering without my reauthorization. The administrative regulation remains in effect should these revisions occur.			
Approved By:	Nancy Newton, City Manager	**Dates:**	Sept. 25, 2020
Author:	Brandt Melick, Information Technology Director		
Responsible Party:	Information Technology (IT)		
Replaces:	N/A		

PERIODIC REVIEW:

Reviewer:		**Date:**	
Reviewer:		**Date:**	
Reviewer:		**Date:**	
Reviewer:		**Date:**	
Reviewer:		**Date:**	

REVISIONS:

Version **#2:**	**Responsible Party:**			
	Revised By:			
	Approved By:		**Date:**	
	Reason/Summary of Changes:			